U

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/755,520	01/05/2001	Heiko H. Ludwig	CH9-1999-0042	5060

7590 04/26/2005	EXAMINER
Anne Vachon Dougherty	BACKER, FIRMIN
3173 Cedar Road	
Yorktown Heights, NY 10598	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 04/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary		Application No.	Applicant(s)
		09/755,520	LUDWIG ET AL.
		Examiner	Art Unit	
		Firmin Backer	3621	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2005* .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____ .

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) ☐ Notice of Informal Patent Application (PTO-152)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .	6) ☐ Other: .

Response to Arguments

1.   Applicant's arguments with respect to claims 1-36 have been considered but are moot in

view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

3.   Claims 1-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rowney et al

(U.S. Patent No. 5,996,076) in view of Sudia et al (U.S. PG Pub No. 2002/0029337 A1)

4.   As per claims 1, 6, 11, 16, 27 and 32, Rowney et al teach a computerized method having

a process flow operating over a computer network comprising a plurality of interconnected

computers and a plurality of resources, each computer including a processor, memory and

input/output devices, each resource operatively coupled to at least one of the computers and

executing at least one of the activities in the process flow, the method comprising extracting

verifiable role certificates from said electronic authorization; and verifying whether role

certificates, associated with the authorization, are themselves authentic (*see fig 1C, 4, 12A, 12B,*

15B, 16, 26, 30, 35, column 15 lines 10-16 line 33, 17 lines 8-18 line 34). Rowney et al fail to

teach an inventive concept of an electronic representation of the transaction and at least one

verifiable anonymous role certificate for each role for which approval is required to be

completed to obtain authorization of the transaction and certificates generated for authentication

completion. However, Sudia et al teach an inventive concept of an electronic representation of

the transaction and at least one verifiable anonymous role certificate for each role for which

approval is required to be completed to obtain authorization of the transaction and certificates

generated for authentication completion (*see abstract, paragraphs 0018, 0042, 0043, 0051,*

0052, 0060). Therefore, it would have been obvious to one of ordinary skill in the art at the time

the invention was made to modify the inventive concept of Rowney et al to include Sudia et al's

electronic representation of the transaction and at least one verifiable anonymous role certificate

for each role for which approval is required to be completed to obtain authorization of the

transaction and certificates generated for authentication completion because this would have

been desirable to use digital signature and certificate mechanisms to encode industry-wide

security policy and authorization information into the signatures and certificates in order to

permit the verifier of a signature to decide whether to accept the signature or certificate as valid,

thus accommodating and easing electronic commerce business transactions.

5.   As per claims 2, 7, 12, 17, 28 and 33, Rowney et al teach a computerized method wherein

roles associated with the role certificates are hashed and compared with hashed roles in a

database of hashed roles (*see fig 1C, 4, 12A, 12B, 15B, 16, 26, 30, 35, column 15 lines 10-16 line*

33, 17 lines 8-18 line 34).

6.   As per claims 3, 8, 13, 18, 29 and 34, Rowney et al teach a computerized method wherein

the authorization is further insured by verifying that role certificates associated with the

authorization correspond with roles in a permission set of roles of an authorization structure, the

role certificates of which being required to authorize the transaction (*see fig 1C, 4, 12A, 12B,*

15B, 16, 26, 30, 35, column 15 lines 10-16 line 33, 17 lines 8-18 line 34).

7.   As per claims 4, 9, 14, 19, 30 and 35, Rowney et al teach a computerized method wherein

the authorization structure is an authorization tree (*see fig 1C, 4, 12A, 12B, 15B, 16, 26, 30, 35,*

column 15 lines 10-16 line 33, 17 lines 8-18 line 34).

8.   As per claims 5, 10, 15, 20, 31 and 36, Rowney et al teach a computerized method

wherein the roles are extracted from the role certificates associated with the transaction, each

extracted role being hashed and these hashed roles being concatenated and hashed again, and

then concatenated with hashes of other permission sets, if any, according to the authorization

structure and hashed once again, resulting in a computed hash value which may be compared to

that which was signed by the Transaction Administrator, a match indicating that the transaction

is authorized (*see fig 1C, 4, 12A, 12B, 15B, 16, 26, 30, 35, column 15 lines 10-16 line 33, 17*

lines 8-18 line 34).

9.   As per claims 21 and 24, Rowney et al teach a Transaction Authorization Method

encoded on a computer readable medium, the method having the following steps receiving a

request for a transaction, obtaining an electronic representation of a document having details of

the transaction from a Digital Document Database returning the transaction details to the

requester awaiting and receiving from the requester the completed representation, signed by the

requester requesting the Authorization Structure for the transaction from the Authorization

Structure Database, the Authorization Structure being pre-signed with a signature by the

Transaction Administrator and verifying the signature, and choosing a permission set of role

names and user members of the permission set to contact to sign in these role names forwarding

details of the transaction request with the signature of the requester to others having roles

corresponding to the chosen permission set and collecting signatures of each role indicated in the

permission set, requesting role certificates from the Role Certificate Database and signatures for

each member of the permission set and encoding the same on the document; and forwarding the

completed electronic document including the signatures and role certificates to the requester, the

document including authorization details required in order to confirm the validity of the

transaction (*see fig 1C, 4, 12A, 12B, 15B, 16, 26, 30, 35, column 15 lines 10-16 line 33, 17 lines

8-18 line 34)*. Rowney et al fail to teach an inventive concept of obtaining the role certificate

signed with a signature by a Transaction Administrator from a Role Certificate Database and

verifying the signature and certificates generated for authentication completion. However, Sudia

et al teach an inventive concept of obtaining the role certificate signed with a signature by a

Transaction Administrator from a Role Certificate Database and verifying the signature and

certificates generated for authentication completion, (*see abstract, paragraphs 0018, 0042, 0043,

0051, 0052, 0060)*. Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify the inventive concept of Rowney et al to include Sudia et

al's electronic representation of obtaining the role certificate signed with a signature by a

Transaction Administrator from a Role Certificate Database and verifying the signature and

certificates generated for authentication completion, because this would have been desirable to

use digital signature and certificate mechanisms to encode industry-wide security policy and

authorization information into the signatures and certificates in order to permit the verifier of a

signature to decide whether to accept the signature or certificate as valid, thus accommodating

and easing electronic commerce business transactions.

10.   As per claims 22 and 25, Rowney et al teach a Transaction Authorization Method

wherein the role certificates and the Authorization Structure consist of hashed information about

permission sets and roles, such hashed information substituting for the unhashed role certificates

and permission sets (*see fig 1C, 4, 12A, 12B, 15B, 16, 26, 30, 35, column 15 lines 10-16 line 33,

17 lines 8-18 line 34*).

11.   As per claims 23 and 26, Rowney et al teach a Transaction Verification Method encoded

on a computer readable medium, the method having the following, using a verification key of the

Role Authority to check each certificate on the document, in the following manner, checking the

signatures on the transaction details using the verification keys in the supplied role certificates

extracting the named roles from the role certificates hashing the roles using a hash-of-hashes

process, checking the computed hash value of the transaction against that was originally signed

by the Transaction Authority to ensure that it is equal to the value for the transaction received in

the Authorization Structure, using the output of the hash-of-hashes process as input to check the

signature on the hash-of-hashes process; if the produced hash-of-hashes string matches the

hashed string signed by the Transaction Authority, then assuming that the request is authorized;

and reporting the result (see fig 1C, 4, 12A, 12B, 15B, 16, 26, 30, 35, column 15 lines 10-16 line

33, 17 lines 8-18 line 34). Rowney et al fail to teach an inventive concept of receiving an

electronic document representing a transaction, associated transaction details being signed by a

Transaction Authority, a collection of role certificates certifying named roles signed by a Role

Authority, the transaction details signed by each of the signing keys corresponding to the

verification keys in the role certificates, and the Authorization Structure and certificates

generated for authentication completion. However, Sudia et al teach an inventive concept of

receiving an electronic document representing a transaction, associated transaction details being

signed by a Transaction Authority, a collection of role certificates certifying named roles signed

by a Role Authority, the transaction details signed by each of the signing keys corresponding to

the verification keys in the role certificates, and the Authorization Structure and certificates

generated for authentication completion, (see abstract, paragraphs 0018, 0042, 0043, 0051,

0052, 0060). Therefore, it would have been obvious to one of ordinary skill in the art at the time

the invention was made to modify the inventive concept of Rowney et al to include Sudia et al's

receiving an electronic document representing a transaction, associated transaction details being

signed by a Transaction Authority, a collection of role certificates certifying named roles signed

by a Role Authority, the transaction details signed by each of the signing keys corresponding to

the verification keys in the role certificates, and the Authorization Structure and certificates

generated for authentication completion, because this would have been desirable to use digital

signature and certificate mechanisms to encode industry-wide security policy and authorization

information into the signatures and certificates in order to permit the verifier of a signature to
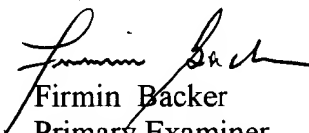
decide whether to accept the signature or certificate as valid, thus accommodating and easing

electronic commerce business transactions.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The

examiner can normally be reached on Mon-Thu 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, James Trammell can be reached on (703) 305-9768. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firmin Backer
Primary Examiner
Art Unit 3621

April 20, 2005